# Exhibit 47

**Excerpts of Gregory Rattray**
**Expert Report**

**IN THE UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF NEW YORK**

| | | |
|---|---|---|
| SECURITIES AND EXCHANGE COMMISSION, | ) | |
| Plaintiff, | ) | |
| v. | ) | Civil Action No. 1:23-cv-09518-PAE-BCM |
| SOLARWINDS CORP. and TIMOTHY G. BROWN, | ) | |
| Defendants. | ) | |

# EXPERT REPORT OF GREGORY RATTRAY
# NOVEMBER 22, 2024

**EXHIBIT 1**
Rattray
2/12/2025
Jessica Waack, CSR
RDR, CRR, NYACR, NYRCR

standard security practices throughout the software development process."[294] I disagree with this opinion.

183. Mr. Graff's analysis and the documents he cites do not support his conclusions. The Security Statement represented that SolarWinds followed a software development lifecycle with a "defined methodology for developing secure software" that incorporated security testing throughout the process.[295] As explained earlier, based on the artifacts and testimony I reviewed, including in particular the FSRs and results of vulnerability scans and penetration tests during the Relevant Period, those representations were clearly true.[296]

184. Mr. Graff again ignores the most pertinent artifacts and testimony and instead tries to extrapolate broadly from a small number of documents about marginal issues. None of these events or documents on which Mr. Graff relies changes any of my opinions because they do not undermine the evidence showing that SolarWinds built security into its software development lifecycle as the Security Statement describes.

### 1. SolarWinds Maintained Separate Development and Production Environments

185. Mr. Graff starts by making an argument that does not even relate to SolarWinds' software development lifecycle, i.e., to the steps that engineers follow in developing software. He instead challenges the Security Statement's representation that "SolarWinds maintains separate development and production environments."[297] That is an issue relating to the company's network security, not its software development lifecycle—which is why it appears under the heading "Network Security" in the Security Statement.[298]

---

[294] *Id.*

[295] SW-SEC00466129 at -132.

[296] *See supra* Section V.F.

[297] Graff Report ¶ 150.

[298] SW-SEC00466129.

186. Specifically, the separation of development and production environments refers to the separation of the part of a company's network where engineers develop software—the "development environment"—from the part of a company's network used to run its day-to-day operations—its "production environment" (which can also be referred to as its "corporate" environment). As noted in the guidance cited by Mr. Graff, separating these two environments is important from a network-security perspective, because development environments "are often configured less securely than production environments," in order to give software engineers the flexibility they need to test software under various conditions.[299] That creates the risk that "attackers may use this difference to discover shared weaknesses or as an avenue for exploitation"[300]; in other words, if there is no separation between development and production systems, an attacker that compromises a less securely configured development system could use it as a vector for penetrating the company's network more broadly. Therefore, it is considered best practice to logically separate a company's development environment from its production environment, by segregating them into different network zones, with a firewall sitting between them that restricts traffic from one entering into the other.

187. This is what the Security Statement represented SolarWinds did. It stated:

> SolarWinds maintains separate development and production environments. Our next generation firewalls (NGFWs) provide adequate network segmentation through the establishment of security zones that control the flow of network traffic. These traffic flows are defined by strict firewall security policies.[301]

In other words, the Security Statement represented that it separated the company's development and production environments by establishing a separate network zone for each and regulating the

---

[299] Graff Report ¶ 143(a) n.270 (quoting OWASP, Secure Coding Practices: Quick Reference Guide, November 2010, at 11); *see also id.* (quoting NIST SP 800-53, at 98 for the statement that "the management of development or test configurations requires greater flexibility").

[300] *Id.*

[301] SW-SEC00466129 at -131.

flow of traffic between them through the use of a next-generation firewall. The firewall would help to prevent an attacker from jumping from the development environment into the production environment.

188. I note that this representation is not among the representations in the Security Statement that the SEC challenges in its Amended Complaint. Nonetheless, for purposes of responding to Mr. Graff's argument, I have reviewed evidence relating to this representation and, based on the evidence I have reviewed, it was true. Multiple witnesses testified that the company had separate network zones for its development environment and its production (or "corporate") environment, and that it used firewalls to separate the two.[302] Moreover, I have reviewed a sample of SolarWinds' firewall logs that were preserved from the Relevant Period, which show "DEV" and "CORP" as two different zones from which traffic is hitting the firewall, and various policies or "rules" regulating the flow of traffic between the two zones.[303] This is clear evidence that SolarWinds logically segregated the two environments through the use of a firewall, exactly as the Security Statement described.[304]

---

[302] *See* E. Quitugua Inv. Tr. at 134:9-136:22 ("[T]here's two domains at SolarWinds, a DEV domain and a TUL domain. One is considered production, and one's considered development. … Q. Okay. And so for example, between the DEV and the TUL domains, was there a firewall used to segment those two network zones? A. Yes."); T. Brown Dep. Tr. at 104:9-14 ("Q. What is your understanding of what it means to have separate development and production environments? A. There were multiple high-level network zones that were in place - so a development zone, a production zone, a lab zone, and then additional kind of microsegmented areas within the network."); *id.* at 105:4-6 (explaining that the company used "Palo Alto Nextgen firewalls" to separate the zones); B. Cline Dep. Tr. at 81:7-83:18 ("Q. … You're saying there's – there's a separate product development environment and a separate standard corporate production environment? A. Correct. … . Q. … So how do you know that SolarWinds maintains separate development and production environments? A. As mentioned, we managed a lot of the firewall rules that would have controlled those environments.").

[303] SW-SEC-SDNY_00055443—SW-SEC-SDNY_00055444.

[304] I also note that that the SARF forms distinguish between an "Active Directory TUL account"—"TUL" was another term used to refer to the production environment—and an "Active Directory SWDEV account," and indicate that, while all users would receive an "Active Directory TUL account," only certain types of employees would receive an "Active Directory SWDEV account." *See, e.g.*, PWC-SEC-00025433 at -434 (listing "Active Directory TUL account" among standard system accesses for all employees, but "Active Directory SWDEV account" for only certain roles). This indicates that separate instances of Active Directory were set up for the development and production environments, which is consistent with the environments being maintained as two separate network zones.

189. Mr. Graff does not genuinely argue otherwise. Instead, he focuses, again, on the email chain from November 2019 discussed above, about SolarWinds developers conducting testing on live billing data in the company's production environment, [305] and he concludes from this that SolarWinds failed to segregate its development and production environments.[306] Mr. Graff is conflating two very different issues. The fact that, for this particular project, SolarWinds developers were testing billing data *inside* the production environment (i.e., inside CORP) does not imply that SolarWinds did not logically segregate that environment from its development environment (i.e., DEV). They were still two separate zones, with a firewall between them.[307] Therefore, the more loosely configured infrastructure within the DEV environment was not a threat to the CORP environment, as it might be if there were no separation between the two. In other words, an attacker still could not exploit weaknesses in machines in the DEV environment as an avenue for attacking machines in the CORP environment.

190. Instead, all that was happening here was that developers were working *inside* the production environment. They weren't disabling the firewall between the production environment and exposing it to threats from the infrastructure in the development environment; they were simply logged into the production environment—with its more securely configured infrastructure—and testing a billing application on live data in that environment. Now, as I discussed earlier, this did pose a potential risk: The developers might accidentally modify the billing data, which, because it was live data, might cause inaccuracies in billing or financial

---

[305] *See supra* ¶¶ 121-126.

[306] Graff Report ¶¶ 150-162.

[307] *See* B. Cline Dep. Tr. at 83:13-84:1 ("[Q.] So how do you know that SolarWinds maintains separate development and production environments? A. As mentioned, we managed a lot of the firewall rules that would have controlled those environments.").

reporting.[308] But that risk has nothing to do with any network-security concern about failing to segregate the DEV and CORP environments.

191. This is yet another example of Mr. Graff focusing on a one-off incident, which he misinterprets to begin with, and trying to make very broad generalizations that are simply unwarranted—all while ignoring far more direct evidence of the practices at issue. In short, Mr. Graff points to no evidence showing that SolarWinds failed to segregate its development environment from its production environment through the use of a firewall, as stated in the Security Statement. It clearly did that. The incident he points to is instead a red herring involving a distinct—and minor—issue. If anything, it only underscores that there *was* a development environment separate from the production environment. The very reason the incident arose was that, while software would typically be tested in the (segregated) development environment, it was not feasible to do so for the billing system at issue—which is why the developers sought a special exemption allowing them to work directly in the production environment instead.[309]

### 2. The Security Statement Did Not Represent Anything About How SolarWinds Developed Internal Software Applications

192. Mr. Graff next opines that the Security Statement's representation that SolarWinds followed secure software development practices was inaccurate because software applications that SolarWinds built for its own *internal* use were not by default subject to the same development practices as the software it built and sold to customers.[310] The Security Statement does not even speak to this issue, however.

193. The Security Statement's representations about the company's software development lifecycle are about the processes it followed in developing the *products* it sold to

---

[308] *See supra* ¶¶ 123-125.

[309] *See* SW-SEC00254254 at -265 (explaining that "[t]he developers are developing in Production as the staging/dev environments are not suitable"). That was a judgment call Mr. Brown was entitled to make.

[310] *See* Graff Report ¶ 163.

receiving and responding to penetration tests from customers was good practice, not evidence that it failed to do penetration testing itself.

216. In sum, I do not believe that Mr. Graff has offered any evidence that calls into question the accuracy of the Security Statement's representations about its software development lifecycle and his report therefore does nothing to change my opinions in that regard.

Signed on December 30, 2024, in Andover, New Jersey.

Greg Rattray